苏 州 大 学 实 验 报 告

院、系	计算机学院	姓名	朱金涛	学号	2327406014
课程名称	计算机网络				
指导教师	高国举	实验完成日期		2025 年 10 月 21 日	

实验名称： IEEE802 标准和以太网

一.实验目的

1. 掌握以太网的报文格式
2. 掌握 MAC 地址的作用
3. 掌握 MAC 广播地址的作用
4. 掌握 LLC 帧报文格式
5. 掌握协议编辑器和协议分析器的使用方法
6. 掌握协议栈发送和接收以太网数据帧的过程

二.实验步骤

练习 1：领略真实的 MAC 帧

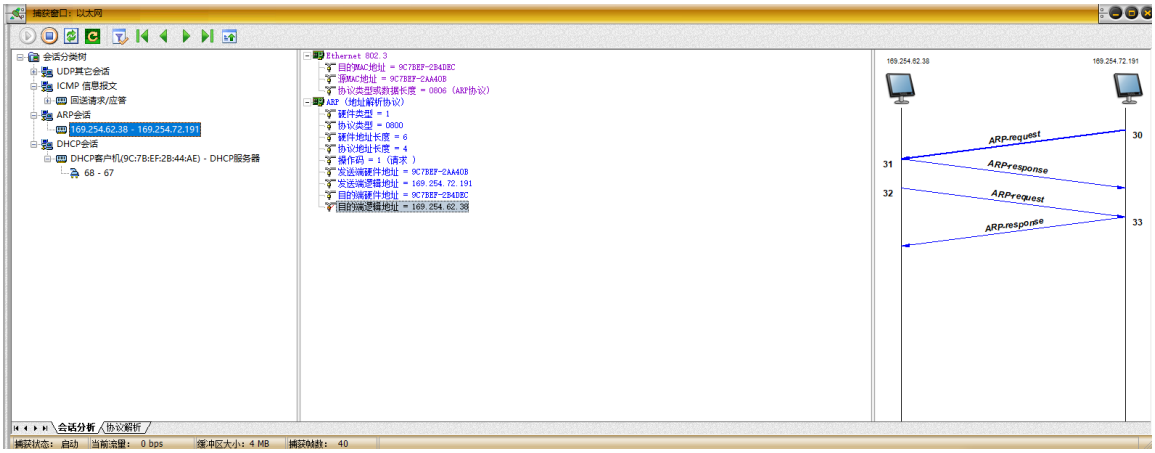
各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。本练习将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

1. 主机 B 启动协议分析器，新建捕获窗口进行数据捕获并设置过滤条件（提取 ICMP 协议）。

对于过滤器的定义：勾选 ETHER 以及 IPv4 当中的 ICMP 选项。

2. 主机 A ping 主机 B，查看主机 B 协议分析器捕获的数据包，观察、记录并分析 MAC 帧格式。

● 记录实验结果



主机 E（本机）收到来自主机 E 的 ICMP 报文，并且观察到正常的请求与回复。

以太网头部(14 bytes)

- Destination MAC
- Source MAC
- Type = 0x0806 (ARP)

ARP 数据结构

- Hardware Type
- Protocol Type
- Hardware Size
- Protocol Size
- Opcode = 1 (request)
- Sender MAC
- Sender IP
- Target MAC (00:00:00:00:00:00)
- Target IP

MAC 层：提供源、目的 MAC 地址

Type 字段：标识使用 ARP 协议

ARP 部分携带 IP ↔ MAC 映射请求

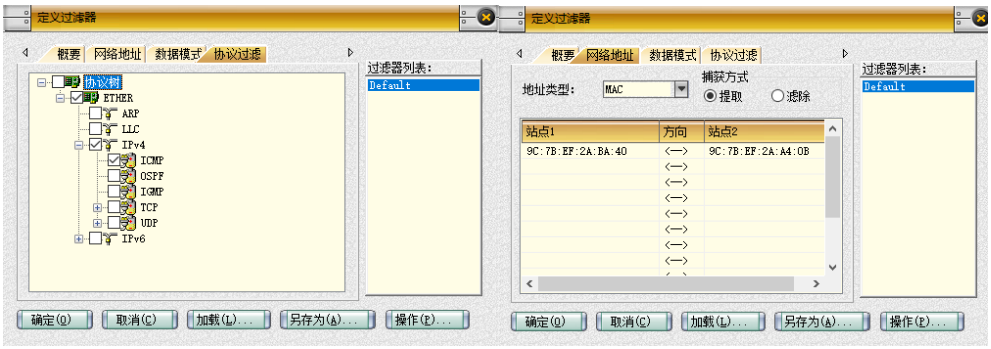
这是一个典型的 ARP 请求帧

3. 将主机 B 的过滤器恢复为默认状态。

练习 2：理解 MAC 地址的作用

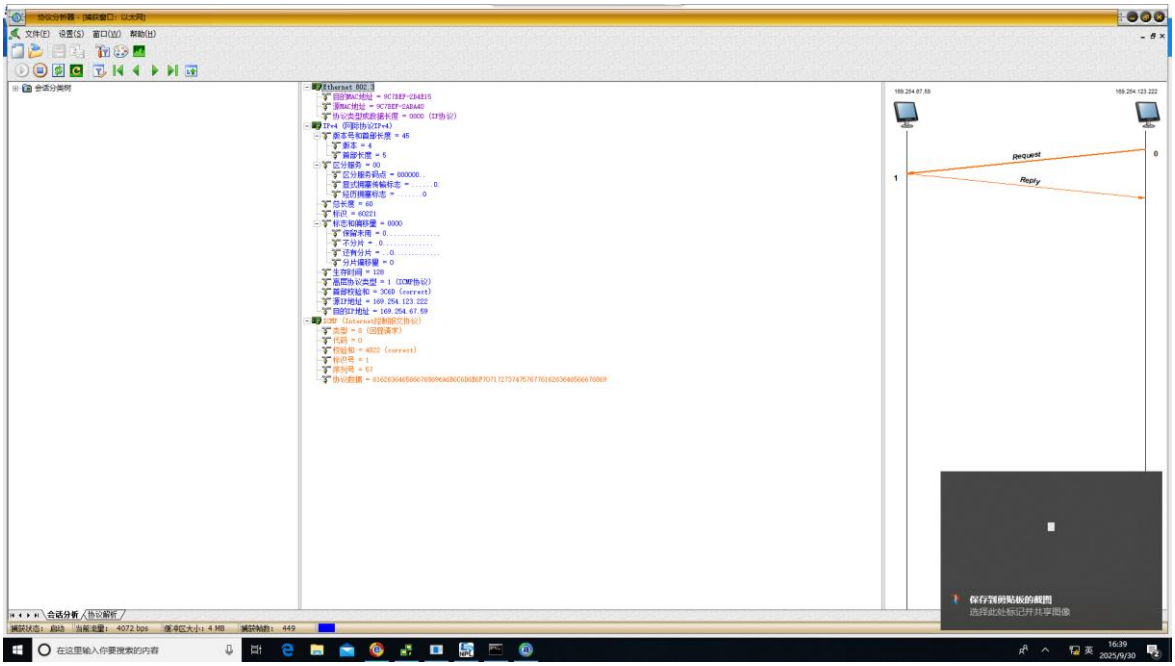
本练习将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 为例，其他组的操作参考主机 A、B 的操作。

1. 主机 B 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（源 MAC 地址为主机 A 的 MAC 地址）。



2. 主机 A ping 主机 B。

3. 主机 B 上停止捕获数据，在捕获的数据中查找主机 A 所发送的 ICMP 数据帧，并分析该帧内容。



这是一个 ICMP Echo Request（Ping 请求）帧，由 IPv4 协议封装并通过以太网发送。

数据结构如下：

Ethernet → MAC 地址、类型 = 0x0800

IPv4 → TTL=128, protocol=ICMP(1)

ICMP → Type=8 (Echo Request), Seq=57

Payload → “abcdefghijklmnopqrstuvwxyz...”

● 记录实验结果（选一栏进行作答）

	本机 MAC 地址	源 MAC 地址	目的 MAC 地址	是否收到，为什么
主机 B	9C:7B:EF:24:BE:15	9C:7B:EF:2A:40:0B	9C:7B:EF:24:BE:15	收到。因为 A 与发送方 B 在同一子网内。

练习 3：编辑并发送 MAC 广播帧

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

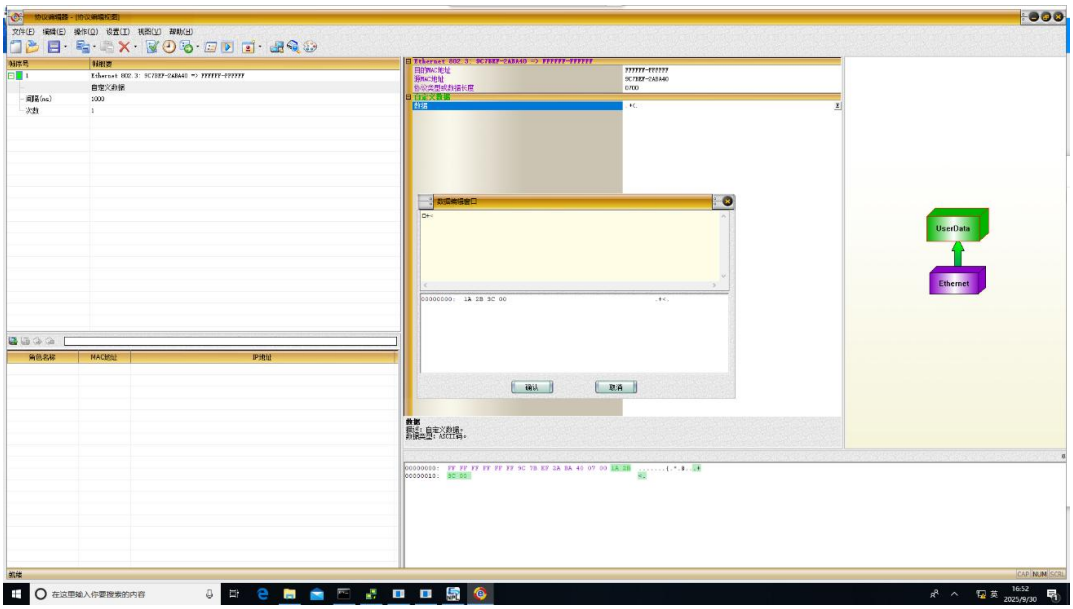
1. 主机 E 启动协议编辑器。
2. 主机 E 编辑一个 MAC 帧：

   目的 MAC 地址：FFFFFF-FFFFFF

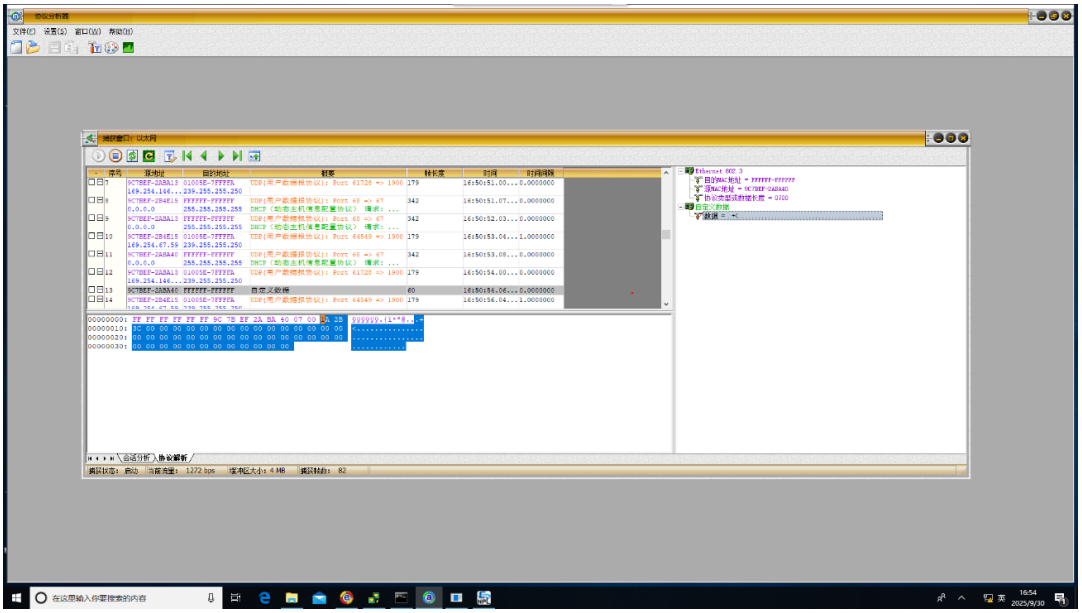
   源 MAC 地址：主机 E 的 MAC 地址

   协议类型或数据长度：大于 0x0600

   数据字段：编辑长度在 46—1500 字节之间的数据



3. 主机 A、B、C、D、F 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（源 MAC 地址为主机 E 的 MAC 地址）。
4. 主机 E 发送已编辑好的数据帧。
5. 主机 A、B、C、D、F 停止捕获数据，查看捕获到的数据中是否含有主机 E 所发送的数据帧。



● 结合练习三的实验结果，简述 FFFFFF-FFFFFF 作为目的 MAC 地址的作用。

上图为本机（E）捕获到的广播帧，其他计算机收到的广播帧均与之相似。

综合实验结果，FFFFFF-FFFFFF 作为目的 MAC 地址表示将帧发送到网络中的所有网卡上，进行广播通信，因此网络中的其余主机（A、B、C、D、F）都能接收到广播帧。

练习 4：编辑并发送 LLC 帧

本练习将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

1. 主机 A 启动协议编辑器，并编写一个 LLC 帧。

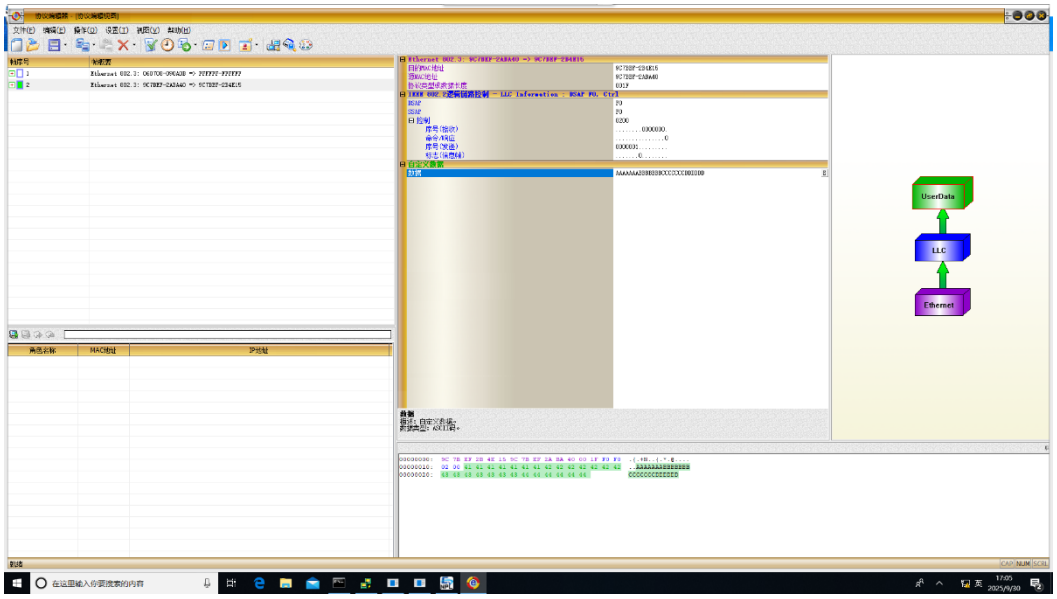
   目的 MAC 地址：主机 B 的 MAC 地址

   源 MAC 地址：主机 A 的 MAC 地址

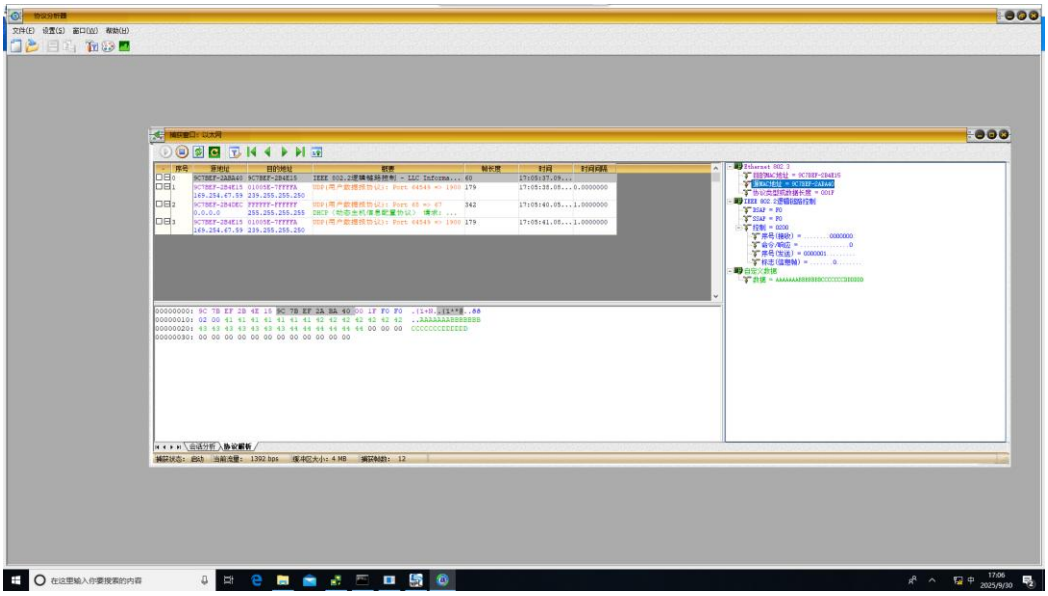
   协议类型和数据长度：001F

   控制字段：填写 02（注：回车后变成 0200，该帧变为信息帧，控制字段的长度变为 2 字节）

   用户定义数据/数据字段：AAAAAAABBBBBBBCCCCCCCDDDDDD（注：长度为 27 个字节）



2. 主机 B 启动协议分析器并开始捕获数据。
3. 主机 A 发送编辑好的 LLC 帧。
4. 主机 B 停止捕获数据，在捕获到的数据中查找主机 A 所发送的 LLC 帧，分析该帧内容。



捕获到的主机 A 发送的 LLC 帧是：

Frame Type：I-Frame（信息帧）

LLC 控制字段：02 00

发送序号 N(S) = 1

接收序号 N(R) = 0

数据区为："AAAAAAABBBBBBBCCCCCCCDDDDDDD"

- 记录实验结果

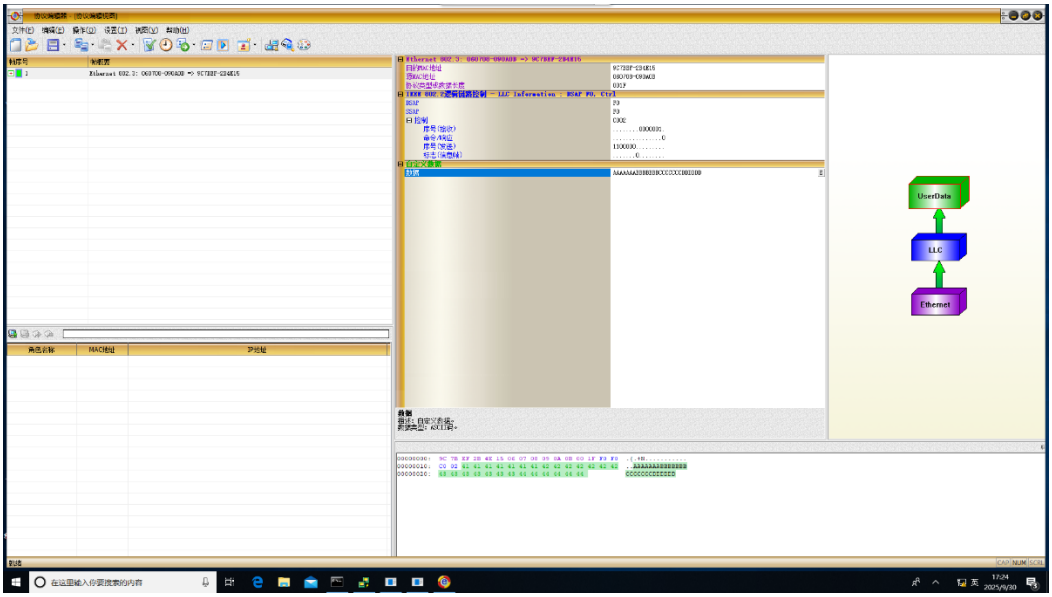
帧类型	发送序号 N（S）	接受序号 N（R）
信息帧（I）	1	0
无编号帧	—	—

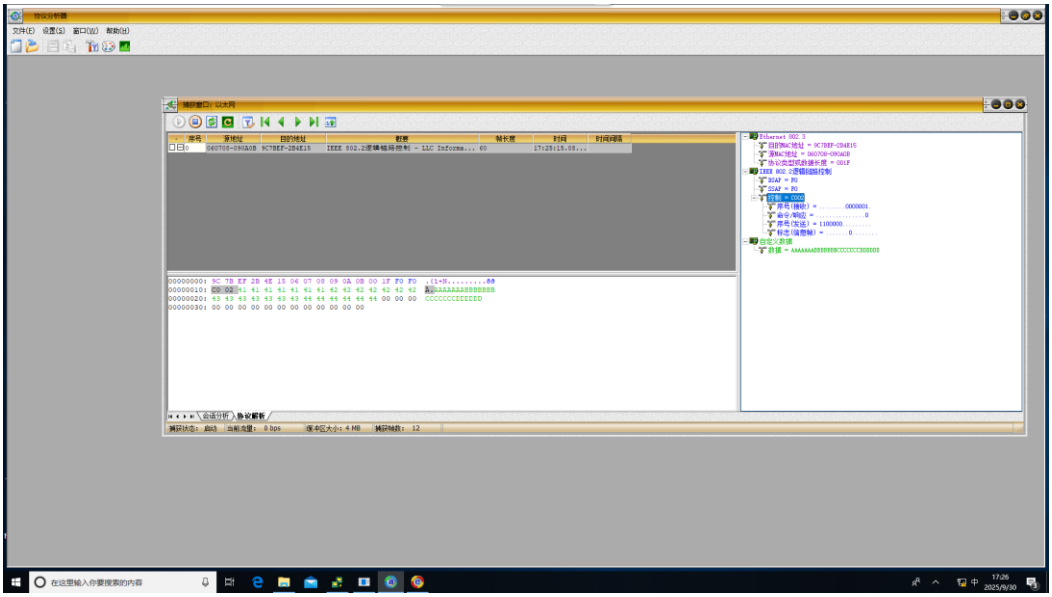
- 简述“协议类型和数据长度”字段的两种含义。

➢ 当字段值 **≤1500（十进制）** 时，表示 **数据长度（Length）**，用于 IEEE 802.3 帧。

➢ 当字段值 **≥1536（0x0600）** 时，表示 **上层协议类型（Type）**，用于以太网 II 型帧。

5. 将第 1 步中主机 A 已编辑好的数据帧修改为“无编号帧”(前两个比特为 1)，用户定义数据/数据字段修改为 AAAAAAABBBBBBBCCCCCCCDDDDDDD（长度为 28 个字节），重做第 2、3、4 步。





该帧是基于 IEEE 802.3/802.2 标准的以太网信息帧（I 帧），源 MAC 为 9C7BEF-2B4E15、目的 MAC 为 060708-090A0B，LLC 子层 DSAP 和 SSAP 均为 F0，LLC 控制字段 C0 02，发送序号 N (S) 为 96、接收序号 N (R) 为 1，数据部分为自定义 AAAAAAABBBBBBBCCCCCCCDDDDDDD。

帧类型	发送序号 N（S）	接受序号 N（R）
信息帧	96	1

三.实验总结与收获

对于练习 1（内容：在协议分析器里抓取同网段通信的以太网/802.3 帧，逐字段核对目的/源 MAC、Type/Length、数据载荷及是否有填充，实际看到当该字段值≤1500 时被解析为长度（802.3），≥0x0600 时被解析为上层协议类型（Ethernet II，如 0x0800→IPv4），并注意到短帧会被自动补齐以满足最小 64 字节；感悟：教材里的“双语义”和“最小帧长”在抓包上都有证据，后续手工构帧时必须保证长度自洽、别被默认值误导）。练习 2（内容：把过滤规则改为按源 MAC，先放宽再收紧，在主机 A→B 的连通性测试中，同一二层广播域内主机能抓到相应二层帧，域外主机抓不到；一开始我因过滤过窄“看不到包”，改回按源 MAC 后恢复；感悟：二层基于 MAC 的转发与广播域边界非常直观，排障经验是“先宽后窄、逐步定位”，比一上来精准过滤更可靠）。练习 3（内容：在协议编辑器手工构造目的 MAC 为 FF:FF:FF:FF:FF:FF 的广播帧，控制好数据长度/必要填充后发送，多台同域主机同时按源 MAC 过滤均能捕获该帧；感悟：广播的域内泛洪效果一目了然，也提醒真实网络要用 VLAN/抑制策略控制广播范围与风暴风险）。练习 4（内容：先在主机 A 拼 **LLC 信息帧** I-Frame：Type/Length 设为 0x001F、控制字段输入 0x02 后自动扩展为两字节 0x0200、数据 27 字节，主机 B 抓包显示字段与填写一致，序号解析为 N(S)=0、N(R)=0；随后改为 LLC 无编号帧 U-Frame（前两比特为 11），数据 28 字节，抓包识别为 U 帧且不含序号，记录为 “—/—”；同时我反复把 Type/Length 设为 ≤1500 与 ≥0x0600 交替发送，验证分析器对长度/类型两种语义的切换一致；感悟：LLC 的控制字段位宽与 I/U 帧差异、序号含义以及 Type/Length 分界都被自己的报文“对拍”确认，今后用 Scapy 等脚本化构帧会更有把握）。

总体而言，我从“看真实帧—用过滤定位—自己构帧再回看”的闭环里把关键概念都落到证据上，既巩固了理论，也形成了可复现的操作与排障思路。